2 GENERAL EMPLOYEE POLICIES

2.7 Privacy Policy

[SEC Regulation S-P]

Information regarding customer accounts for individuals is subject to SEC Regulation S-P "Privacy Of Consumer Financial Information." This section explains employees' obligation to maintain the privacy of information. A section *Customer Privacy Policies And Procedures* in the chapter *COMMUNICATIONS WITH THE PUBLIC* outlines firm procedures.

1. Regulation S-P requirements apply to individual and not institutional accounts and include U.S. and foreign accounts.
2. Protected information is termed "nonpublic personal information." This is information obtained by BOKFS that is not deemed "public information" which is defined as information that may be obtained from three sources: federal, state or local government records; widely distributed media; or disclosures to the general public that are required to be made by federal, state, or local law.
3. At the time an account is opened the customer is provided with BOKFS' privacy policy and is given the opportunity to opt out of arrangements to share nonpublic information with nonaffiliated third parties. The privacy policy is also provided to customers on an annual basis.
4. Employees are prohibited from sharing or releasing nonpublic personal information other than to authorized parties. This includes a prohibition against:
    - Sending internal reports or other information about firm customers to a non-affiliated 3rd party (unless authorized).
    - Sending internal or other documents that include customer nonpublic information to your personal e-mail address.

Questions about providing customer information should be referred to Compliance.

2.7.1 BOKFS Privacy Policy

The BOKFS Privacy Policy is saved to the Retail Documents SharePoint site and can be accessed at this link: BOKFS Privacy Policy

2 GENERAL EMPLOYEE POLICIES

2.20 Computer Records, Equipment And Software

Responsibility	• Designated Supervisor (Sales Supervisors) • Compliance - lost devices or breach of data • Bank
Resources	• Disks and other computer records maintained by a terminating employee • Reports of lost devices
Frequency	• As required
Action	• Bank: Provide employees with education and policy information about proper use of computer and other electronic equipment including appropriate security measures and accessing customer information • Bank: Instruct offices to secure equipment and information • Designated Supervisor: Secure disks, computers, software, and other firm property when an employee terminates • Designated Supervisor: Do not permit removal of firm equipment without approval • Contact Compliance: Take action regarding lost devices including remote deactivation, if available, and assessment of whether a breach of customer information has or may occur
Record	• Inform Bank and CCO if device is lost or breached and there is a possibility that material information can be accessed by non-employees

Nothing in this manual related to computer records, equipment, and software is meant to replace or overrule the policies and procedures listed in the Corporate Information Security Program Policy ("ISPP") . Refer to the ISPP for more detailed information regarding how BOKFS manages the security of our information assets. (https://spfarm.bok.com/sites/PolicyAdministration/Policies%20and%20Procedures/Forms/End%20User.aspx -> Information Security -> Critical policies)

BOKFS considers its computer records, systems, and software to be corporate assets. Employees are responsible for protecting these assets from unauthorized use, destruction, or unauthorized modification. This includes a prohibition against violating copyright laws or licensing agreements applicable to computer software.

Physical equipment (PCs, printers, software, diskettes, *etc.*) must be placed in a secure location to avoid theft, tampering, unauthorized use, and environmental hazards (water, smoke, magnets, *etc.*). The use of personal computers for BOKFS business is subject to the same guidelines and restrictions as BOKFS computers.

When an employee terminates, any disks or other storage medium that includes proprietary information, including customer information, are considered property of BOKFS and must be left with BOKFS.

2.20.1 Laptop Computers And Other Mobile Devices

Employees who use laptops or other mobile devices for Firm business are responsible for the security of the device and the information contained on it. Serious security breaches can occur if a device containing or capable of accessing confidential information is lost or stolen.

Employees who use laptops for company business are required to comply with requirements provided by the Bank.

2.20.2 Reporting Lost Devices

- The loss of a mobile device **must be immediately reported to Compliance**.

2.20.3 Identifying And Reporting Data Breaches

- All employees are required to immediately report an identified potential intrusion into a mobile device or into BOKFS' systems.

2.20.4 Software

Software installed and used on electronic devices is limited to software approved by BOKFS. BOKFS will install or provide authorized software for business use including anti-virus and anti-malware protection.

Employees are strictly prohibited from installing software other than what is authorized by BOKFS.

2.20.5 Prohibited Downloading

Employees are prohibited from:

- Downloading customer and other confidential firm information from BOKFS' mainframe or other central records, unless specifically authorized
- Using portable devices such as USB key drives, MP3 players, mobile phones, and other devices for downloading information unless specifically authorized
- Downloading programs from the Web to BOKFS computers unless specifically authorized